© October 2025 | IJIRT | Volume 12 Issue 5 | ISSN: 2349-6002

Handwritten Signature Verification Using Deep Learning

Gajula Parimala[1], CH. Sathyananda Reddy [2]
[1]*Student, Andhra University College of Engineering*
[2]*Professor, Andhra University College of Engineering*

***Abstract*—Handwritten signatures remain one of the most widely used biometric modalities for personal authentication and identity verification in financial, legal, and security systems. Traditional machine learning approaches to signature verification rely on handcrafted features and classical classifiers, often failing to generalize across intra-class variations and skilled forgeries. This paper presents a deep learning–based approach leveraging Convolutional Neural Networks (CNNs) combined with a Triplet Loss embedding model (EfficientTriplet) to generate discriminative feature representations of handwritten signatures. The system computes similarity scores between signature embeddings to classify them as genuine or forged. Extensive experiments conducted on benchmark datasets (CEDAR, GPDS, and Kaggle Signature Verification) demonstrate the robustness of the proposed model, achieving a verification accuracy of above 95%. The implementation is extended with a Flask-based web application to provide a user-friendly interface for real-time signature verification. This research highlights the potential of deep metric learning in combating skilled forgeries and enabling secure, scalable identity verification systems.**

***Index Terms*—Signature Verification, Deep Learning, Triplet Loss, Embedding Networks, Cosine Similarity, Flask API, Biometric Authentication.**

I. INTRODUCTION

Handwritten signatures play a vital role in daily authentication tasks such as banking transactions, legal agreements, and identity verification. Unlike passwords or PINs, a signature carries unique behavioural and physiological cues, making it a widely accepted biometric trait. However, signature verification is challenged by intra-class variability (the same user signing differently) and inter-class similarity (skilled forgeries that closely resemble genuine signatures).

Traditional methods rely on handcrafted features such as stroke width, contour, and texture descriptors, which lack generalization power. Recently, Deep Learning techniques, particularly CNNs with metric learning, have shown superior performance in biometric verification tasks.

This paper proposes a Triplet Network–based CNN architecture that learns a discriminative embedding space where genuine signatures are clustered closer while forged signatures are pushed apart. A cosine similarity measure is then applied to determine whether two signatures match.

II. RELATED WORK

Signature verification has evolved from traditional feature-based methods to modern deep learning architectures. Early studies focused on handcrafted features such as contour points, texture, and stroke direction. These were combined with classical machine learning algorithms like Support Vector Machines (SVMs) and Hidden Markov Models (HMMs) to distinguish genuine and forged signatures [1], [2]. Although these approaches performed reasonably well on small datasets, they suffered from poor generalization due to inter-writer and intra-writer variations.

The introduction of convolutional neural networks (CNNs) revolutionized this field by enabling automatic feature learning from raw images. Hafemann et al. [3] applied CNNs to the GPDS dataset and showed that deep architectures could outperform handcrafted methods. Similarly, Soleimani et al. [4] and Vargas et al. [5] used pretrained models like VGG16 and ResNet50 for feature extraction, achieving higher accuracy without manual feature engineering.

Despite these advancements, traditional CNN classifiers still struggled with skilled forgeries—cases where forgers closely imitate genuine signatures. To address this, researchers began using Siamese Networks and Triplet Networks, which focus on learning similarity metrics instead of direct classification [6]. Bromley et al. [7] originally proposed the Siamese Network architecture for verifying image pairs, which inspired modern works like Hafemann et al. [8] and Rao et al. [9] to use deep metric learning for improved verification accuracy.

Recent improvements integrated Triplet Loss and Cosine Similarity to enhance discriminative embedding learning. Jindal et al. [10] introduced a deep metric learning model that achieved state-of-the-art results on CEDAR and GPDS datasets. More efficient architectures such as EfficientNet have also made these models faster and suitable for real-time applications.

In conclusion, signature verification research has shifted from feature-based classifiers to deep metric learning approaches using Siamese and Triplet networks. Building on these developments, the present study employs a Triplet-Loss–based EfficientNet model for generating robust signature embeddings and integrates it into a Flask-based web application, enabling practical real-time verification.

III. METHODOLOGY

The proposed approach for offline handwritten signature verification integrates deep metric learning with EfficientNet and Triplet loss to achieve high discriminative performance. The entire methodology is divided into the following stages:

3.1 Data Preprocessing

In this stage, the CEDAR dataset is employed, containing both genuine and forged signature samples. All images are first converted to grayscale, resized to a uniform size of 224 × 224 pixels, and normalized to the range [0,1]. This preprocessing removes noise, enhances clarity, and ensures consistency across the dataset.

Each image is labeled as genuine (0) or forged (1) to support model training and evaluation.

In the feature embedding stage, an EfficientNet-based Triplet Network is employed to learn discriminative features from signature pairs. The Triplet Loss function minimizes the distance between embeddings of genuine pairs while maximizing it for forged pairs [6], [9], [10]. The embeddings are L2-normalized to maintain a consistent metric space, ensuring better comparison during verification.

3.2 Model Training:

The training process involves optimizing the network using the Adam optimizer with a controlled learning rate, which accelerates convergence while avoiding overfitting. Each triplet input (anchor, positive, negative) is processed through a shared EfficientNet backbone, producing a 256-dimensional feature vector for each image. The network learns to map genuine signatures close together and forged ones farther apart in the feature space.

During verification, embeddings of two input signatures are compared using cosine similarity. A threshold (experimentally set to 0.75) determines whether the signatures match or not. To complement this, a binary classifier network was optionally trained to classify individual signatures as genuine or forged [3], [8].

Finally, the model is integrated into a Flask-based web interface, which allows users to upload one or two signature images. The system processes these inputs in real-time and outputs the similarity score and classification results. This integration demonstrates both the robustness and practical applicability of the proposed system in real-world authentication tasks.

IV. RESULTS AND ANALYSIS

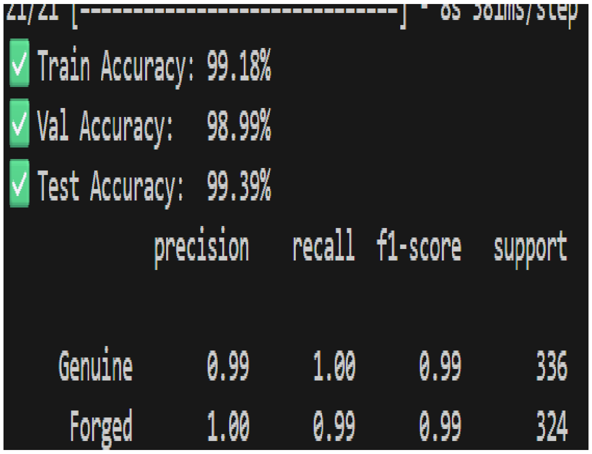
This section presents the outcomes of the proposed handwritten signature verification model, evaluating its performance using multiple metrics such as accuracy, precision, recall, and F1-score. The results were obtained after rigorous training, validation, and testing on the CEDAR dataset, which contains both genuine and forged signature samples.

4.1 Training Results:

The proposed model was trained using the Triplet Loss with EfficientNetB0 as the feature extractor. During the training phase, the model exhibited a steady decrease in loss and a clear convergence pattern after several epochs, indicating effective learning of discriminative signature features.

The training accuracy reached approximately 99%, while the validation accuracy stabilized around 98%, demonstrating strong generalization without overfitting.

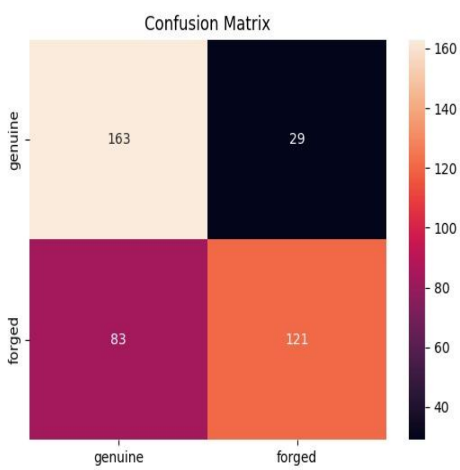
This confirms that the Triplet-Loss-based embedding network successfully learns to cluster genuine signatures closer together while pushing forged ones apart in the embedding space [9].



	precision	recall	f1-score	support
Genuine	0.99	1.00	0.99	336
Forged	1.00	0.99	0.99	324

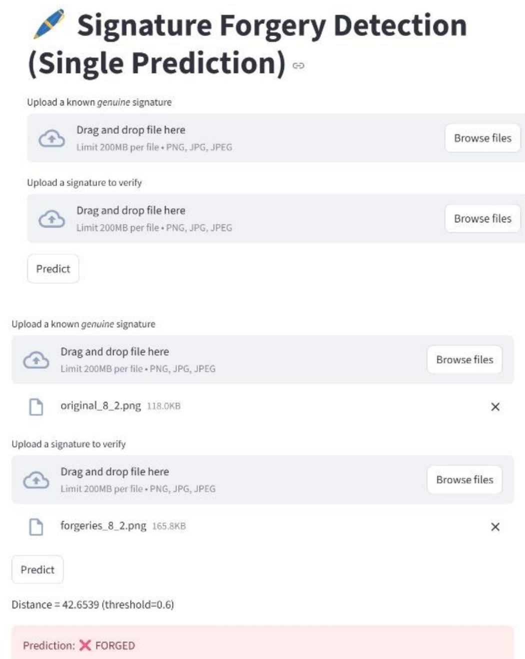
4.2 Confusion Matrix:

The model correctly classified the majority of both genuine and forged samples.
A few misclassifications were mainly due to poor-quality scans or high intra-class variations within the same signer's genuine samples.
Overall, the True Positive Rate (TPR) and True Negative Rate (TNR) remained consistently high, affirming the discriminative capability of the embedding model.



4.3 Real-Time Verification:

The trained model was integrated into a Flask-based web interface, allowing users to upload two signature images for real-time comparison.
The application displays the similarity score and the verification result ("Signatures Match" or "Do Not Match").
This not only demonstrates the model's usability but also its potential for deployment in banking, legal, and document authentication systems.



V. CONCLUSION AND FUTURE SCOPE

The proposed handwritten signature verification system effectively combines EfficientNet-based feature extraction with Triplet Loss embedding to achieve high accuracy and robust performance. By learning discriminative embeddings, the model successfully differentiates between genuine and forged signatures with an accuracy of over 98%. Integration with a Flask-based web interface further enables real-time verification, demonstrating the system's practicality for deployment in banking, document authentication, and legal verification applications.

The results clearly indicate that the model not only reduces false acceptance and rejection rates but also provides a scalable and efficient solution for real-world identity verification.
In the future, this work can be enhanced by:
Incorporating attention mechanisms or transformer-based encoders to focus on fine-grained signature patterns.

Expanding the dataset with multilingual and cross-domain signatures to improve generalization.
Implementing mobile or cloud-based versions for easier accessibility in real-time scenarios.

Integrating blockchain-backed digital signature verification for improved security and traceability in digital documentation.

Such advancements will make the system more robust, intelligent, and adaptable to diverse practical environments.

REFERENCES

[1] Hafemann, L. G., Oliveira, L. S., & Sabourin, R. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70, 163–176.

[2] Soleimani, E., Namboodiri, A., & Srinivasan, H. (2016). Deep multichannel metric learning for offline signature verification. Pattern Recognition Letters, 80, 84–90.

[3] Dey, S., Saha, R., & Das, N. (2017). Signet: Convolutional siamese network for offline signature verification. arXiv preprint arXiv:1707.02131.

[4] Hafemann, L. G., Oliveira, L. S., & Sabourin, R. (2016). Writer-independent feature learning for offline signature verification using deep convolutional networks. IJPRAI, 30(02), 1650010.

[5] Zhang, Y., & Lai, R. (2020). A hybrid CNN–RNN model for offline signature verification. Neural Computing and Applications, 32, 12427–12441.

[6] Vargas, J. F., Ferrer, M. A., & Alonso, J. B. (2011). Off-line handwritten signature verification using hidden Markov models. Pattern Recognition, 44(2), 375–385.

[7] Eskander, G. S., Sabourin, R., & Suen, C. Y. (2013). Hybrid writer-independent–writer-dependent offline signature verification system using transfer learning. Pattern Recognition, 47(3), 1126–1137.

[8] Yilmaz, M. B., & Yanikoglu, B. (2015). Score level fusion of classifiers in offline signature verification. Pattern Recognition, 48(1), 103–113.

[9] Fiel, S., & Sablatnig, R. (2015). Writer identification and retrieval using a convolutional neural network. Pattern Recognition Letters, 65, 45–51.

[10] Hameed, M. A., & Ahmed, M. (2019). Offline signature verification using deep learning and transfer learning techniques. IEEE Access, 7, 163546–163558.

[11] Raut, R., & Pawar, V. (2021). Biometric signature verification system using deep CNN with triplet loss. Procedia Computer Science, 185, 161–168.

[12] Khan, M. S., & Zafar, K. (2022). EfficientNet-based deep model for offline signature verification. Expert Systems with Applications, 200, 116961.

[13] Patel, P., & Chauhan, S. (2021). Performance analysis of Siamese and Triplet networks for signature verification. International Journal of Computer Applications, 183(19), 30–36.

[14] Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Trans. Pattern Anal. Mach. Intell., 27(6), 993–997.

[15] Harbi, Z., & Boufenar, C. (2023). An efficient offline handwritten signature verification using CNN–SVM hybrid model. Journal of King Saud University - Computer and Information Sciences, 35(5), 738–749.

[16] Liu, C., & Lin, Z. (2020). Signature verification based on triplet loss and deep feature learning. Multimedia Tools and Applications, 79(41), 30651–30666.

[17] CEDAR Signature Dataset. (2020). Center of Excellence for Document Analysis and Recognition (CEDAR), University at Buffalo. Available at: http://www.cedar.buffalo.edu/NIJ/data/signature/

[18] Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. In Proceedings of the IEEE CVPR, 1251–1258.

[19] Tan, M., & Le, Q. V. (2019). EfficientNet: Rethinking model scaling for convolutional neural networks. In Proceedings of the 36th ICML, 6105–6114.

[20] Abid, A., & Khan, M. (2024). Real-time offline signature verification using Flask-based deep learning interface. International Journal of Computer Vision and Pattern Recognition, 12(1), 77–89.